Switch 24 portů bez PoE

Specifikace hardware switch 24 x 1GbE port	Ano/Ne
Základní vlastnosti	
Třída zařízení přepínač, dostupné typy stejné série: 24x 10/100/1000 BaseT RJ45	
min 2x SFP+ (1/10GE) uplink	
Rozměry 1U Rack mount	
Aktivní chlazení	
Napájení 230V	
Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa atd	
VS backplane kapacity min. 80Gbps	
VS min. počet switchů = 4	
Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3 min. 128 Gbps / 95Mpps	
Musí umožňovat redundantní VS backplane / forwarding plane	
Redundantní VS Control Plane (master a backup switch)	
Switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
Fyzické Interface, podpora	
1GE interface UNI	
10/100/1000BaseT	
1GE interface NNI	
1000BASE-T	
1000BASE-SX	
1000BASE-LX	
1000BASE-LH (nebo ZX)	
10GE interface NNI	
10GBASE-SR	
10GBASE-LRM	
10GBASE-LR	
10GBASE-ER	
L2 funkce	
Min. 16k MAC na systém	
Jumbo frames 9k jako minimum	
VLAN id rozsah 4k	
konfigurovaných VLAN současně min. 250	
IEEE 802.1Q (trunk intf.)	
Port Based VLAN	
Voice VLAN	
Private VLAN	
Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
LAG (min. 20 skupin) musí být podporováno napříč členy VS	
až 8 LAG členu ve skupině	

LACP	
xSTP (IEEE 802.1D/802.1s/802.1w)	
Kompatibilní s PVSTP+	
STP security funkce	
BPDU guard	
Loop protection	
LLDP (IEEE 802.1AB)	
LLDP-MED (integrace s Voice VLAN)	
ACLs (Access listy) / Policing	
ACL v HW s ohledem na performance specifikaci v A sekci	
Port ACL (vstup / výstup)	
VLAN ACL	
L2-L4 "matching" podmínky	
IPv6 ACL	
L3 funkce	
Podporováno v HW s ohledem na performance	
RVI (Routed VLAN interface)	
IPv4 routes = 500 jako minimum	
Static routing	
DHCP server / relay	
Multicast	
Podporováno v HW	
IGMP snooping v1/2/3	
Protokol IPv6	
Podpora VRRP nebo ekvivalentní pro IPv6	
Podpora OSPFv3	
Podpora IPv6 ACL	
Podpora DHCPv6 snooping	
Podpora IPv6 ND inspection	
Podpora IPv6 MLD snooping	
Bezpečnost	
802.1x "single / multiple / single secured supplicant"	
802.1x static bypass	
802.1x VLAN assignment	
802.1x MAC radius	
VoIP VLAN s 802.1x spoluprací	
DHCP snooping	
DHCP untrust porty	
Dynamic ARP inspection	
Static MAC / MAC limitation per port	
MAC move limit	
Policing / rate limit pro provoz směrem k CPU	
ACLka na provoz směrem k CPU	
Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
Klasifikace provozu	

Podporováno v HW	
„ Trust“ Klasifikace provozu na 802.1p, DSCP, IP prec	
„Untrust“ Klasifikace provozu na L2-L4 polích hlavičky paketu	
Egress Port shaping	
Ingress Policing	
Min. 4x Queues na port	
Scheduling mechanismus DWRR per port	
Min. 2 priority per Scheduler	
Strict priority implementace (LLQ)	
Rewrite rules – přepsání CoS bitů	
Management	
cli interface dostupný lokálně, telnet, SSH	
user authentication (local, Radius, TACACS+)	
Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
Možnost konfiguračních změn přes txt soubor	
podpora syslog (local, remote syslog server)	
možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
SNMP verze 1/2c/3	
Ping, traceroute	
Flow technologie (sFlow nebo Netflow nebo IPfix) prosím specifikujte technologii	
Traffic mirroring (local / remote mirroring)	
Správa revizí konfigurací	
Vynucení potvrzení změn nastavení	
Dostupný centrální management s GUI pro správu min. 100 přepínačů	
Shodný management s ostatními přepínači a firewallem nabídky	
Servisní a doplňkové požadavky	
Záruka a produktová podpora min. 5 let Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

Switch 24 portů s PoE

Specifikace hardware switch 24 x 1GbE PoE+ port	Ano/Ne
Základní vlastnosti	
Třída zařízení přepínač, dostupné typy stejné série: 24x 10/100/1000 BaseT PoE+ RJ45	
min 2x SFP+ (1/10GE) uplink	
Rozměry 1U Rack mount	
Aktivní chlazení	
Napájení 230V	
Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa atd	
VS backplane kapacity min. 40Gbps	
VS min. počet switchů = 4	
Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3 min. 128 Gbps / 95Mpps	
Musí umožňovat redundantní VS backplane / forwarding plane	
Redundantní VS Control Plane (master a backup switch)	
Switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
Fyzické Interface, podpora	
1GE interface UNI	
10/100/1000BaseT	
PoE podpora pro PoE varianty na všech interfacech IEEE 802.3af pro všechny PoE porty na switchy současně IEEE 802.3at min pro polovinu PoE portů na switchy současně	
1GE interface NNI	
1000BASE-T	
1000BASE-SX	
1000BASE-LX	
1000BASE-LH (nebo ZX)	
10GE interface NNI	
10GBASE-SR	
10GBASE-LRM	
10GBASE-LR	
10GBASE-ER	
L2 funkce	
Min. 16k MAC na systém	
Jumbo frames 9k jako minimum	
VLAN id rozsah 4k	
konfigurovaných VLAN současně min. 250	
IEEE 802.1Q (trunk intf.)	
Port Based VLAN	
Voice VLAN	

Private VLAN	
Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
LAG (min. 20 skupin) musí být podporováno napříč členy VS	
až 8 LAG členu ve skupině	
LACP	
xSTP (IEEE 802.1D/802.1s/802.1w)	
Kompatibilní s PVSTP+	
STP security funkce	
BPDU guard	
Loop protection	
LLDP (IEEE 802.1AB)	
LLDP-MED (integrace s Voice VLAN)	
ACLs (Access listy) / Policing	
ACL v HW s ohledem na performance specifikaci v A sekci	
Port ACL (vstup / výstup)	
VLAN ACL	
L2-L4 "matching" podmínky	
IPv6 ACL	
L3 funkce	
Podporováno v HW s ohledem na performance	
RVI (Routed VLAN interface)	
IPv4 routes = 500 jako minimum	
Static routing	
DHCP server / relay	
Multicast	
Podporováno v HW	
IGMP snooping v1/2/3	
Protokol IPv6	
Podpora VRRP nebo ekvivalentní pro IPv6	
Podpora OSPFv3	
Podpora IPv6 ACL	
Podpora DHCPv6 snooping	
Podpora IPv6 ND inspection	
Podpora IPv6 MLD snooping	
Bezpečnost	
802.1x "single / multiple / single secured supplicant"	
802.1x static bypass	
802.1x VLAN assignment	
802.1x MAC radius	
VoIP VLAN s 802.1x spoluprací	
DHCP snooping	
DHCP untrust porty	
Dynamic ARP inspection	
Static MAC / MAC limitation per port	
MAC move limit	
Policing / rate limit pro provoz směrem k CPU	
ACLka na provoz směrem k CPU	

Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
Klasifikace provozu	
Podporováno v HW	
„ Trust“ Klasifikace provozu na 802.1p, DSCP, IP prec	
„Untrust“ Klasifikace provozu na L2-L4 polích hlavičky paketu	
Egress Port shaping	
Ingress Policing	
Min. 4x Queues na port	
Scheduling mechanismus DWRR per port	
Min. 2 priority per Scheduler	
Strict priority implementace (LLQ)	
Rewrite rules – přepsání CoS bitů	
Management	
cli interface dostupný lokálně, telnet, SSH	
user authentication (local, Radius, TACACS+)	
Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
Možnost konfiguračních změn přes txt soubor	
podpora syslog (local, remote syslog server)	
možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
SNMP verze 1/2c/3	
Ping, traceroute	
Flow technologie (sFlow nebo Netflow nebo IPfix) prosím specifikujte technologii	
Traffic mirroring (local / remote mirroring)	
Správa revizí konfigurací	
Vynucení potvrzení změn nastavení	
Dostupný centrální management s GUI pro správu min. 100 přepínačů	
Shodný management s ostatními přepínači a firewallem nabídky	
Servisní a doplňkové požadavky	
Záruka a produktová podpora min. 5 let Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

Switch 48 portů Bez PoE

Specifikace hardware switch 48 x 1GbE port	Ano/Ne
Základní vlastnosti	
Třída zařízení přepínač, dostupné typy stejné série: 48x 10/100/1000 BaseT RJ45	
min 2x SFP+ (1/10GE) uplink	
Rozměry 1U Rack mount	
Aktivní chlazení	
Napájení 230V	
Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa atd	
VS backplane kapacity min. 80Gbps	
VS min. počet switchů = 4	
Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3 min. 176 Gbps / 130Mpps	
Musí umožňovat redundantní VS backplane / forwarding plane	
Redundantní VS Control Plane (master a backup switch)	
Switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
Fyzické Interface, podpora	
1GE interface UNI	
10/100/1000BaseT	
PoE podpora pro PoE varianty na všech interfacech IEEE 802.3af pro všechny PoE porty na switchy současně IEEE 802.3at min pro polovinu PoE portů na switchy současně	
1GE interface NNI	
1000BASE-T	
1000BASE-SX	
1000BASE-LX	
1000BASE-LH (nebo ZX)	
10GE interface NNI	
10GBASE-SR	
10GBASE-LRM	
10GBASE-LR	
10GBASE-ER	
L2 funkce	
Min. 16k MAC na systém	
Jumbo frames 9k jako minimum	
VLAN id rozsah 4k	
konfigurovaných VLAN současně min. 250	
IEEE 802.1Q (trunk intf.)	
Port Based VLAN	
Voice VLAN	

Private VLAN	
Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
LAG (min. 20 skupin) musí být podporováno napříč členy VS	
až 8 LAG členu ve skupině	
LACP	
xSTP (IEEE 802.1D/802.1s/802.1w)	
Kompatibilní s PVSTP+	
STP security funkce	
BPDU guard	
Loop protection	
LLDP (IEEE 802.1AB)	
LLDP-MED (integrace s Voice VLAN)	
ACLs (Access listy) / Policing	
ACL v HW s ohledem na performance specifikaci v A sekci	
Port ACL (vstup / výstup)	
VLAN ACL	
L2-L4 "matching" podmínky	
IPv6 ACL	
L3 funkce	
Podporováno v HW s ohledem na performance	
RVI (Routed VLAN interface)	
IPv4 routes = 500 jako minimum	
Static routing	
DHCP server / relay	
Multicast	
Podporováno v HW	
IGMP snooping v1/2/3	
Protokol IPv6	
Podpora VRRP nebo ekvivalentní pro IPv6	
Podpora OSPFv3	
Podpora IPv6 ACL	
Podpora DHCPv6 snooping	
Podpora IPv6 ND inspection	
Podpora IPv6 MLD snooping	
Bezpečnost	
802.1x "single / multiple / single secured supplicant"	
802.1x static bypass	
802.1x VLAN assignment	
802.1x MAC radius	
VoIP VLAN s 802.1x spoluprací	
DHCP snooping	
DHCP untrust porty	
Dynamic ARP inspection	
Static MAC / MAC limitation per port	
MAC move limit	
Policing / rate limit pro provoz směrem k CPU	

ACLka na provoz směrem k CPU	
Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
Klasifikace provozu	
Podporováno v HW	
„ Trust“ Klasifikace provozu na 802.1p, DSCP, IP prec	
„Untrust“ Klasifikace provozu na L2-L4 polích hlavičky paketu	
Egress Port shaping	
Ingress Policing	
Min. 4x Queues na port	
Scheduling mechanismus DWRR per port	
Min. 2 priority per Scheduler	
Strict priority implementace (LLQ)	
Rewrite rules – přepsání CoS bitů	
Management	
cli interface dostupný lokálně, telnet, SSH	
user authentication (local, Radius, TACACS+)	
Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
Možnost konfiguračních změn přes txt soubor	
podpora syslog (local, remote syslog server)	
možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
SNMP verze 1/2c/3	
Ping, traceroute	
Flow technologie (sFlow nebo Netflow nebo IPfix) prosím specifikujte technologii	
Traffic mirroring (local / remote mirroring)	
Správa revizí konfigurací	
Vynucení potvrzení změn nastavení	
Dostupný centrální management s GUI pro správu min. 100 přepínačů	
Shodný management s ostatními přepínači a firewallem nabídky	
Servisní a doplňkové požadavky	
Záruka a produktová podpora min. 5 let	
Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

Switch 48 portů s PoE

	Specifikace hardware switch 48 x 1GbE port	Ano/Ne
	Základní vlastnosti	
	Třída zařízení přepínač, dostupné typy stejné série: 48x 10/100/1000 BaseT PoE+ RJ45	
	min 2x SFP+ (1/10GE) uplink	
	Rozměry 1U Rack mount	
	Aktivní chlazení	
	Napájení 230V	
	Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa atd	
	VS backplane kapacity min. 80Gbps	
	VS min. počet switchů = 4	
	Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3, kapacita min. 176 Gbps / 130Mpps	
	Musí umožňovat redundantní VS backplane / forwarding plane	
	Redundantní VS Control Plane (master a backup switch)	
	Switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
	Fyzické Interface, podpora	
	1GE interface UNI	
	10/100/1000BaseT	
	PoE podpora pro PoE varianty na všech interfacech IEEE 802.3af pro všechny PoE porty na switchy současně IEEE 802.3at min pro polovinu PoE portů na switchy současně	
	1GE interface NNI	
	1000BASE-T	
	1000BASE-SX	
	1000BASE-LX	
	1000BASE-LH (nebo ZX)	
	10GE interface NNI	
	10GBASE-SR	
	10GBASE-LRM	
	10GBASE-LR	
	10GBASE-ER	
	L2 funkce	
	Min. 16k MAC na systém	
	Jumbo frames 9k jako minimum	
	VLAN id rozsah 4k	
	konfigurovaných VLAN současně min. 250	
	IEEE 802.1Q (trunk intf.)	
	Port Based VLAN	
	Voice VLAN	
	Private VLAN	
	Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
	LAG (min. 20 skupin) musí být podporováno napříč členy VS	
	až 8 LAG členu ve skupině	
	LACP	
	xSTP (IEEE 802.1D/802.1s/802.1w)	
	Kompatibilní s PVSTP+	

	STP security funkce	
	BPDU guard	
	Loop protection	
	LLDP (IEEE 802.1AB)	
	LLDP-MED (integrace s Voice VLAN)	
	ACLs (Access listy) / Policing	
	ACL v HW s ohledem na performance specifikaci v A sekci	
	Port ACL (vstup / výstup)	
	VLAN ACL	
	L2-L4 "matching" podmínky	
	IPv6 ACL	
	L3 funkce	
	Podporováno v HW s ohledem na performance	
	RVI (Routed VLAN interface)	
	IPv4 routes = 500 jako minimum	
	Static routing	
	DHCP server / relay	
	Multicast	
	Podporováno v HW	
	IGMP snooping v1/2/3	
	Protokol IPv6	
	Podpora VRRP nebo ekvivalentní pro IPv6	
	Podpora OSPFv3	
	Podpora IPv6 ACL	
	Podpora DHCPv6 snooping	
	Podpora IPv6 ND inspection	
	Podpora IPv6 MLD snooping	
	Bezpečnost	
	802.1x "single / multiple / single secured supplicant"	
	802.1x static bypass	
	802.1x VLAN assignment	
	802.1x MAC radius	
	VoIP VLAN s 802.1x spoluprací	
	DHCP snooping	
	DHCP untrust porty	
	Dynamic ARP inspection	
	Static MAC / MAC limitation per port	
	MAC move limit	
	Policing / rate limit pro provoz směrem k CPU	
	ACLka na provoz směrem k CPU	
	Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
	Klasifikace provozu	
	Podporováno v HW	
	„ Trust“ Klasifikace provozu na 802.1p, DSCP, IP prec	
	„Untrust“ Klasifikace provozu na L2-L4 polích hlavičky paketu	
	Egress Port shaping	
	Ingress Policing	
	Min. 4x Queues na port	
	Scheduling mechanismus DWRR per port	

	Min. 2 priority per Scheduler	
	Strict priority implementace (LLQ)	
	Rewrite rules – přepsání CoS bitů	
	Management	
	cli interface dostupný lokálně, telnet, SSH	
	user authentication (local, Radius, TACACS+)	
	Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
	Možnost konfiguračních změn přes txt soubor	
	podpora syslog (local, remote syslog server)	
	možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
	SNMP verze 1/2c/3	
	Ping, traceroute	
	Flow technologie (sFlow nebo Netflow nebo IPfix) prosím specifikujte technologii	
	Traffic mirroring (local / remote mirroring)	
	Správa revizí konfigurací	
	Vynucení potvrzení změn nastavení	
	Dostupný centrální cloudový management s GUI pro správu min. 100 přepínačů	
	Shodný management s ostatními přepínači a firewallem nabídky	
	Servisní a doplňkové požadavky	
	Záruka a produktová podpora min. 5 let	
	Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

Switch 12 portů s PoE

	Specifikace hardware switch 12 x 1GbE port	Ano/Ne
	Základní vlastnosti	
	Třída zařízení přepínač, dostupné typy stejné série: 12x 10/100/1000 BaseT PoE+ RJ45	
	min 2x SFP+ (1/10GE) uplink	
	Pasivní chlazení	
	Napájení 230V	
	Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa atd	
	VS backplane kapacity min. 40Gbps	
	VS min. počet switchů = 4	
	Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3 min. 64 Gbps / 47Mpps	
	Switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
	Fyzické Interface, podpora	
	1GE interface UNI	
	10/100/1000BaseT	
	PoE podpora pro PoE varianty na všech interfacech IEEE 802.3af pro všechny PoE porty na switchy současně IEEE 802.3at min pro polovinu PoE portů na switchy současně	
	1GE interface NNI	
	1000BASE-T	
	1000BASE-SX	
	1000BASE-LX	
	1000BASE-LH (nebo ZX)	
	10GE interface NNI	
	10GBASE-SR	
	10GBASE-LRM	
	10GBASE-LR	
	10GBASE-ER	
	L2 funkce	
	Min. 16k MAC na systém	
	Jumbo frames 9k jako minimum	
	VLAN id rozsah 4k	
	konfigurovaných VLAN současně min. 250	
	IEEE 802.1Q (trunk intf.)	
	Port Based VLAN	
	Voice VLAN	
	Private VLAN	
	Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
	LAG (min. 8 skupin) musí být podporováno napříč členy VS	
	až 8 LAG členu ve skupině	
	LACP	
	xSTP (IEEE 802.1D/802.1s/802.1w)	
	Kompatibilní s PVSTP+	
	STP security funkce	
	BPDU guard	
	Loop protection	

	LLDP (IEEE 802.1AB)	
	LLDP-MED (integrace s Voice VLAN)	
	ACLs (Access listy) / Policing	
	ACL v HW s ohledem na performance specifikaci v A sekci	
	Port ACL (vstup / výstup)	
	VLAN ACL	
	L2-L4 "matching" podmínky	
	IPv6 ACL	
	L3 funkce	
	Podporováno v HW s ohledem na performance	
	RVI (Routed VLAN interface)	
	IPv4 routes = 500 jako minimum	
	Static routing	
	DHCP server / relay	
	Multicast	
	Podporováno v HW	
	IGMP snooping v1/2/3	
	Protokol IPv6	
	Podpora VRRP nebo ekvivalentní pro IPv6	
	Podpora OSPFv3	
	Podpora IPv6 ACL	
	Podpora DHCPv6 snooping	
	Podpora IPv6 ND inspection	
	Podpora IPv6 MLD snooping	
	Bezpečnost	
	802.1x "single / multiple / single secured supplicant"	
	802.1x static bypass	
	802.1x VLAN assignment	
	802.1x MAC radius	
	VoIP VLAN s 802.1x spoluprací	
	DHCP snooping	
	DHCP untrust porty	
	Dynamic ARP inspection	
	Static MAC / MAC limitation per port	
	MAC move limit	
	Policing / rate limit pro provoz směrem k CPU	
	ACLka na provoz směrem k CPU	
	Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
	Management	
	cli interface dostupný lokálně, telnet, SSH	
	user authentication (local, Radius, TACACS+)	
	Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
	Možnost konfiguračních změn přes txt soubor	
	podpora syslog (local, remote syslog server)	
	možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
	SNMP verze 1/2c/3	
	Ping, traceroute	
	Flow technologie (sFlow nebo Netflow nebo IPfix) prosím specifikujte technologii	

	Traffic mirroring (local / remote mirroring)	
	Správa revizí konfigurací	
	Vynucení potvrzení změn nastavení	
	Dostupný centrální management s GUI pro správu min. 100 přepínačů	
	Shodný management s ostatními přepínači a firewallem nabídky	
	Servisní a doplňkové požadavky	
	Záruka a produktová podpora min. 5 let	
	Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

WiFi AccessPoint (AP)

	Specifikace hardware AP	Ano/Ne
	Základní vlastnosti	
	WiFi standard 802.11ax (WiFi-6) zpětná kompatibilita s 802.11a/b/g/n/ac	
	2,4 Ghz 2x2 : 2 MIMO s přenosem až 550 Mbps data rate	
	4x4 : 4 MIMO s přenosem až 2 400 Mbps data rate	
	Dedikovaná anténa pro 2.4GHz and 5GHz dual-band WIDS/WIPS, spectrum analysis	
	Bluetooth 5.0 anténa	
	Fyzické Interface,	
	1GE interface UNI	
	1x port 10/100/1000BaseT RJ45	
	1x port 100/1000/2500 Base T RJ45	
	IEEE 802.3at PoE Options	
	Reset to the factory default nastavení	
	Management	
	Shodný management s ostatními přepínači a firewallem nabídky	
	Dostupný cloudový centrální management s GUI pro správu min. 500 AP	
	Servisní a doplňkové požadavky	
	Záruka a produktová podpora min. 5 let	
	Zařízení nesmí být výběhový model. (End Of Sale, retired atp.)	

Páteřní switch

Specifikace hardware	Ano/Ne
Základní vlastnosti	
Třída zařízení přepínač, dostupné typy stejné série: min. 24x 1/10GbE Base SFP/SFP+	
min 2x QSFP+ (40GE) zabudované	
Rozměry umístitelný do stojanu	
Redundantní aktivní chlazení	
Napájení 230V st, redundance 1+1	
Seskupení switchů do Virtuálního switche (VS) libovolná kombinace dostupných typů série Chování jednoho Network elementu = MNGT přístup, interface, konfigurace L2/L3, správa	
VS backplane kapacity min. 150Gbps (platné pro switche umožňující VS)	
VS min. počet switchů = 2	
Non-blocking - Line rate switch architektura (započítány VS backplane porty) pro L2/L3	
Redundantní VS backplane / forwarding plane	
Redundantní VS Control Plane (master a backup switch)	
switche ve VS musí být vyměnitelné bez dopadu na zbytek VS HW	
Fyzické Interface, podpora	
1GE interface NNI	
1000BASE-T	
1000BASE-SX	
1000BASE-LX	
1000BASE-LH (nebo ZX)	
10GE interface NNI	
10GBASE-SR	
10GBASE-LRM	
10GBASE-LR	
40GE interface NNI	
40GBASE-SR4	
40GBASE-LR4	
L2 funkce	
Min. 288k MAC na systém	
Jumbo frames 9k jako minimum	
VLAN id rozsah 4k	
konfigurovaných VLAN současně min. 4000	
IEEE 802.1Q (trunk intf.)	
Port Based VLAN	
Voice VLAN	
Private VLAN	
Native VLAN (možnost akceptovat non-tagged paket na trunk portu)	
LAG (min. 80 skupin), musí být podporováno napříč členy VS	
až 8 LAG členu ve skupině	
LACP	
xSTP (IEEE 802.1D/802.1s/802.1w)	

Kompatibilní s PVSTP+	
STP security funkce	
BPDU guard	
Loop protection	
LLDP (IEEE 802.1AB)	
LLDP-MED (integrace s Voice VLAN)	
MACsec (IEEE 802.1AE) – vyžadováno pro všechny 1 GB porty bez omezení	
ACLs (Access listy) / Policing	
ACL v HW s ohledem na performance	
Port ACL (vstup / výstup)	
VLAN ACL	
Router ACL	
L2-L4 "matching" podmínky	
IPv6 ACL	
L3 funkce	
Podporováno v HW s ohledem na performance specifikaci	
RVI (Routed VLAN interface)	
IPv4 routes = 13000 jako minimum	
IPv6 routes = 3000 jako minimum	
Static routing	
Dynamic routing (OSPF, IS-IS, BGP)	
Graceful restart pro OSPF, IS-IS, BGP	
Virtual Routing and Forwarding (VRF, routing instances)	
DHCP server / relay	
Multicast	
Podporováno v HW	
IGMP snooping v1/2/3	
Protokol IPv6	
Podpora VRRP nebo ekvivalentní pro IPv6	
Podpora OSPFv3	
Podpora IPv6 ACL	
Podpora DHCPv6 snooping	
Podpora IPv6 ND inspection	
Podpora IPv6 MLD snooping	
Bezpečnost	
802.1x "single / multiple / single secured supplicant"	
802.1x static bypass	
802.1x VLAN assignment	
802.1x MAC radius	
VoIP VLAN s 802.1x spoluprací	
DHCP snooping	
DHCP untrust porty	
Dynamic ARP inspection	
Static MAC / MAC limitation per port	
MAC move limit	
Policing / rate limit pro provoz směrem k CPU	

ACLka na provoz směrem k CPU	
Možnost automaticky blokovat infikovanou koncovou stanici z prvku centrální správy	
Klasifikace provozu	
Podporováno v HW	
„ Trust“ Klasifikace provozu na 802.1p, DSCP, IP prec	
„Untrust“ Klasifikace provozu na L2-L4 polích hlavičky paketu	
Egress Port shaping	
Ingress Policing	
Min. 8x Queues na port	
Scheduling mechanismus DWRR per port	
Min. 2 priority per Scheduler	
Strict priority implementace (LLQ)	
Rewrite rules – přepsání CoS bitů	
High Availability a modularita	
VRRP	
Management	
cli interface dostupný lokálně, telnet, SSH	
user authentication (local, Radius, TACACS+)	
Automatický backup konfigurace na remote SCP nebo FTP nebo TFTP	
Možnost konfiguračních změn přes txt soubor	
podpora syslog (local, remote syslog server)	
možnost scriptování tcl, python nebo jiný script jazyk - uveďte možnost podmínky (if) a cyklu (for)	
SNMP verze 1/2c/3	
Ping, traceroute	
Flow technologie (sFlow nebo Netflow nebo IPfix)	
Traffic mirroring (local / remote mirroring)	
Správa revizí konfigurací	
Vynucení potvrzení změn nastavení	
Dostupný centrální management s GUI pro správu min. 100 přepínačů	
Shodný management s ostatními přepínači nabídky	
Servisní a doplňkové požadavky	
Záruka a produktová podpora min. 5 let Zařízení nesmí být vyběhový model. (End Of Sale, retired atp.)	

Páteřní firewall

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Typ zařízení	NG firewall	
Formát zařízení	Do racku, max. 1U	
Počet 10Gbe SFP+ portů pro data	Min. 4	
počet datových 1GE + 10G SFP+ portů	16x 1GE 4x 10GE	
Počet portů pro management min 1Gbe	Min. 1	
PoE+ portů	Min. 16	
Propustnost	Min. 10 Gbps	
Propustnost IPS	Min. 2 Gbps	
Propustnost VPN	Min. 3,5 Gbps	
Propustnost NGFW	Min. 1 Gbps	
Max. počet konkurenčních spojení (concurrent sessions)	Min. 380 000	
Rychlost vytváření nových spojení	Min 50 000 / s	
Síťové služby: DNS, DHCP (klient, server), http proxy, ssh proxy, reverzní proxy, FTP gateway	ANO	
Podpora sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	ANO	
Podpora VLAN	ANO, min. 1024 VLAN	
Podpora QoS a shape	ANO	
VPN: site-to-site, IPSec VPN, SSL VPN	ANO	
Podpora vícefaktorového ověřování u SSL VPN	ANO	
Podpora šifrování	Podpora min. IPSec: AES 256, RSA	
Certifikáty	Podpora využití více CA současně	
Aplikační kontrola	Rozpoznávání a kategorizace typů aplikací. Prioritizace trafiku na základě typu aplikace. QoS na základě typu aplikace. Politiky na základě typu aplikace. Detekce aplikace uvnitř SSL komunikace. Možnost nastavování pravidel na základě typu aplikace. URL filtering	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Ověřování uživatelů	Ověřování uživatelů, možnost definovat pravidla na základě uživatele. Podpora napojení a využívání MS AD Podpora preautentikace uživatelů na základě členství v AD skupině (pro reverzní proxy).	
Protokoly	IPv4, IPv6, VOIP (h.232,SIP)	
Routování	BGP, OSFP, RIP, statické routování, routování na základě rozpoznané aplikace, routování na základě politik	
Podpora IPv6 dynamického routování	Ano, min. OSPFv3, BGP	
NAT	sNAT, dNAT, PAT	
Podpora L2 (transparentního) módu s podporou NAT a PAT	ANO	
Podpora L3 (routovaného) módu s podporou NAT a PAT	ANO	
Vysoká dostupnost – cluster	Active/active, active/passive, Transparentní failover bez přerušení session, synchronizace konfigurace	
Vysoká dostupnost – cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	ANO	
Vysoká dostupnost – cluster musí podporovat stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	ANO	
Management	Jednotný management nástroj, konfigurace a správa všech FW, clusterů z jedné konzole. Distribuce konfigurace napříč FW,… Podpora testování pravidel. Pokud je vyžadována dodatečná licence, tak musí být součástí nabídky	
Přístup uživatelů	Ověřování proti MS AD / LDAP	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Napájení a chlazení	Redundantní hotswap zdroje a ventilátory	
Monitoring	Podpora SNMP	
Logování	Podpora SYSLOG, CEF	
Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací apod.	ANO	
Podpora filtrace IPv4, IPv6	ANO	
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	ANO	
Podpora inspekce IPv6 provozu	ANO	
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v internetu	ANO	
Možnost řízení rychlosti datových toků na úrovni pravidel FW	ANO	
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	ANO	
API rozhraní pro sdílení kontextových informací s dalšími systémy	ANO	
IDS/IPS	ANO	
Aktualizace definic IPS v reálném čase	ANO	
Podpora IDS režimu – pasivního monitorování (TAP režim)	ANO	
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí	ANO	
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	ANO	
Podpora 802.1Q tagovaných rámců	ANO	
Podpora různých IPS politik pro různé typy provozu	ANO	
Inspekce pro IPv4 i IPv6	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	ANO	
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	ANO	
Podpora aplikace pro psaní zákaznických filtrů	ANO	
Musí umět detekovat a blokovat útoky průzkumných aktivit	ANO	
Musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	ANO	
Antivirus, antimalware	ANO	
Ochrany proti DoS, DDoS, Spoofing, Flooding, ARP Spoofing a trashing	ANO	
Ochrana proti komunikačním a protokolovým anomáliím	ANO	
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	ANO	
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	ANO	
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	ANO	
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	ANO	
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	ANO	
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	ANO	
Zobrazení pohybu malware – aktivita škodlivého kódu přímo v GUI centralizované konzole	ANO	
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	ANO	
Podpora databází reputací adres v Internetu (Security Intelligence)	ANO	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	ANO	
Podpora pasivního monitorování (TAP režim)	ANO	
Podpora 802.1Q tagovaných rámců	ANO	
Podporovaných aplikací	ANO	
Kategorie aplikací (nebezpečné, důležité, apod.)	ANO	
Kategorizované světové URL s podporou českého Internetu	ANO	
Řízení přístupu k WWW pomocí definice časových kvót pro jednotlivé kategorie	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Filtrace podle typů aplikací webových i ne-webových	ANO	
Filtrace podle reputace serverů	ANO	
SSL inspekce (dekrypce/enkrypce)	ANO	
Databáze známých uzlů botnet sítí C&C	ANO	
Databáze známých adres anonymních proxy, otevřených mail relay	ANO	
Databáze známých nebezpečných URL adres a jmenných domén	ANO	
Filtry mohou zohlednit roli a identitu uživatele	ANO	
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury (tj. odesílání např. netflow, sflow, jflow)	ANO	
Přehled o síťových spojeních má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj – cíl - adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj – cíl - port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikace Množství přenesených dat	
Vzdálená správa přes grafické rozhraní	ANO	
Přístup ke GUI http/https protokolem	ANO	
Možnost vzdáleného přístupu protokolem ssh přímo do FW	ANO	
Možnost přístupu k textovým logům (syslog) přímo ve FW	ANO	
Možnost centrální správy při nasazení více firewallů	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Při centrální správě: možnost sdílených bezpečnostních politik	ANO	
Při použití clusteru se spravuje pouze jeden logický prvek	ANO, min. na úrovni politik	
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, databáze známých hrozeb, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	ANO	
Zobrazení logů a událostí v grafickém rozhraní správy	ANO	
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	ANO	
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	ANO	
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost sdílení politik, centrální sledování zdraví boxů, apod.	ANO	
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	ANO	
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	ANO	
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Uchazeč dle nabízeného zařízení
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	ANO	
Pro reporty lze definovat template definující formát a obsah reportu	ANO	
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	ANO	
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	ANO	
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, apod.	ANO	
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	ANO	
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	ANO	
Podpora sdílení informací se SIEM (např. API rozhraní, syslog apod.)	ANO	
Podpora API pro přístup z externích systémů ke komponentám centralizovaného managementu	ANO	
Podpora API pro možnost využití ovládání firewallu v rámci orchestrace a automatizace nad platformou VMware (vRealize a NSX)	ANO	
Podpora řízeného přístupu podle rolí administrátorů	ANO	
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	ANO	

Centrální Management

	Specifikace	Ano/Ne
	Základní vlastnosti	
	Možnost monitoringu provozu AP, switch a FW	
	Moznost konfigurace AP s pomocí šablon.	
	Moznost konfigurace switche s pomocí šablon.	
	Moznost konfigurace FW s pomocí šablon.	
	Možnost přepsání zděděné konfigurace na zařízení	
	Možnost monitoringu jednotlivého uživatele používajícího infrastrukturu	
	Možnost zpětného monitoringu jednotlivého uživatele až 7 dní zpět	
	Možnost vytváření reportu	
	Audit Log – možnost monitorování činnosti jednotlivých správců	
	Šifrované spojení mezi jednotlivými zařízeními a cloudem	
	V případě ztráty spojení s Cloudovým managementem neomezená funkčnost celého systému.	
	V případě nutnosti možnost vypnutí konfigurace FW přes cloud a provádět konfiguraci lokálně	
	Možnost zasílání informaci a telemetrii zařízením třetích stran přes API rozhraní	