Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

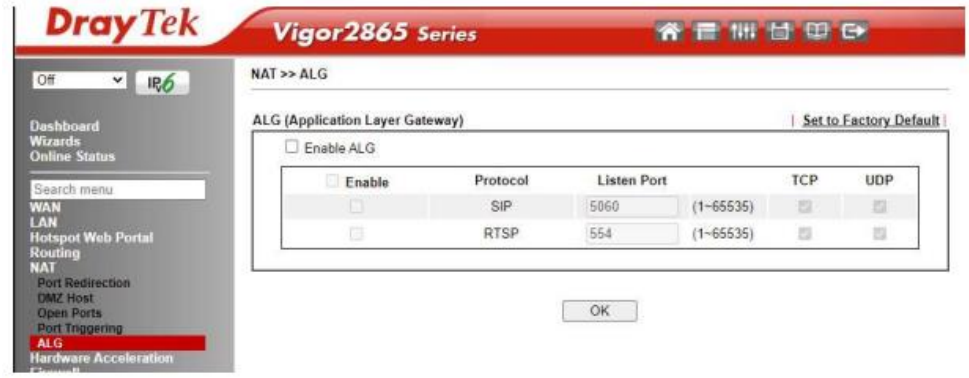
1. Configurazione del NAT (Open Ports)

Nella presente guida rapida viene indicata la modalità più veloce ed efficace per eseguire un NAT con Static Port Mapping con i Router Draytek® e un generico IP PBX on premise (in locale, all'interno della vostra azienda).

L'esempio è riferito al modello Vigor 2865 ma le indicazioni sono applicabili a tutti i modelli Draytek basati su sistema operativo DrayOS. Le Regole ACL presentate sono riferite esplicitamente alle tipologie di account VoIP forniti da VoipVoice.

La modalità più stabile e sicura per configurare un centralino IP, utilizza un NAT di tipo Full Cone con Static Port Mapping e protezioni ACL. Per un corretto funzionamento del protocollo SIP è necessario che le eventuali funzionalità di SIP ALG o SIP HELPER siano disattivate.

La configurazione predefinita di tutti i router Draytek prevede che il SIP ALG sia disattivo. È possibile verificare lo stato del SIP ALG nel menu NAT → ALG. Tutte le opzioni devono rimanere SEMPRE disattivate.



Per eseguire la configurazione delle regole statiche di NAT accedere al menu NAT → Open Ports.

Cliccare sulla prima regola disponibile (nel nostro caso: 1)

Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

COMMENT: Assegneremo a questa prima regola il nome di PBX_LOCAL_NAT

WAN INTERFACE: Selezionare la WAN1 oppure la WAN2 a seconda della WAN utilizzata dal router

SOURCE IP: Selezionare “IP GROUP” e “VOIPVOICE”. Questo filtro, applicato sulle sorgenti IP, costituisce una regola ACL per consentire l’accesso al NAT solamente agli indirizzi IP ricompresi nelle subnet Voipvoice. Fare riferimento al punto 2 della presente guida per creare gli oggetti e i gruppi di oggetti (configurare le ACL).

PRIVATE IP: Digitare o selezionare l’IP LAN utilizzato dal centralino telefonico IP. Nell’esempio si suppone che il centralino Asterisk abbia IP pari a 192.168.1.150.

PORTE: Configura come in figura la regola per la porta SIP - TCP/UDP 5060 e la regola per il range di porte RTP - UDP 10000-20000.

(Le precedenti porte sono state scelte in base all’utilizzo più comune riscontrato nei PBX on-premise, consigliamo di consultare il manuale del prodotto oppure il supporto tecnico del produttore per individuare le porte corrette da abilitare.)

Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

La seguente regola riguarda solo se abbiamo un 3CX on-premise:

Configureremo nella regola precedente per le porte RTP dalla 9000-10999 e poi procediamo con una seconda regola di NAT per la porta relativa al Tunnel 5090 e alla presenza 5001. In questo secondo caso le porte non saranno protette da regole ACL.

Sarà quindi consentito accedere al centralino 3CX da qualunque postazione remota utilizzando l'APP 3CX per Smartphone o il Softphone 3CX per PC Desktop.

COMMENT: Assegneremo a questa prima regola il nome di 3CX_TUN_CON (Tunnel, Webserver, Console e Presenza). L'accesso alla management console può essere limitato successivamente direttamente dalle impostazioni di 3CX, in base a specifici Indirizzi IP.

WAN INTERFACE: Selezionare la WAN1 oppure la WAN2 a seconda della WAN utilizzata dal router

SOURCE IP: Lasciare l'opzione "Any"

PRIVATE IP: Digitare o selezionare l'IP LAN utilizzato dal centralino telefonico 3CX. Nell'esempio si considera che il centralino 3CX abbia IP pari a 192.168.1.250.

PORTE: Configura come in figura la regola per il tunnel 3CX - TCP/UDP 5090 e la regola per webserver e presenza sulla porta TCP 5001

Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

2. Configurazione delle ACL (IP Objects e IP Groups)

Una ACL è una semplice condizione che permette o meno l'accesso ad un determinato sistema informatico. Nel nostro caso, al fine di limitare l'esposizione delle porte del centralino (quelle oggetto di NAT statico), le ACL costituiscono dei filtri basati su Gruppi di Indirizzi IP ai quali è concesso l'accesso NAT al Centralino IP.

Ogni tipologia di account VoIP Voipvoice lavora su una o più subnet IP. In Particolare:

Account VoIP "user.voipvoice.it"

- 62.94.199.32/28 - 83.211.223.192/28 - 83.211.227.0/26 - 83.211.9.160/27

Account VoIP "trunk.voipvoice.it"

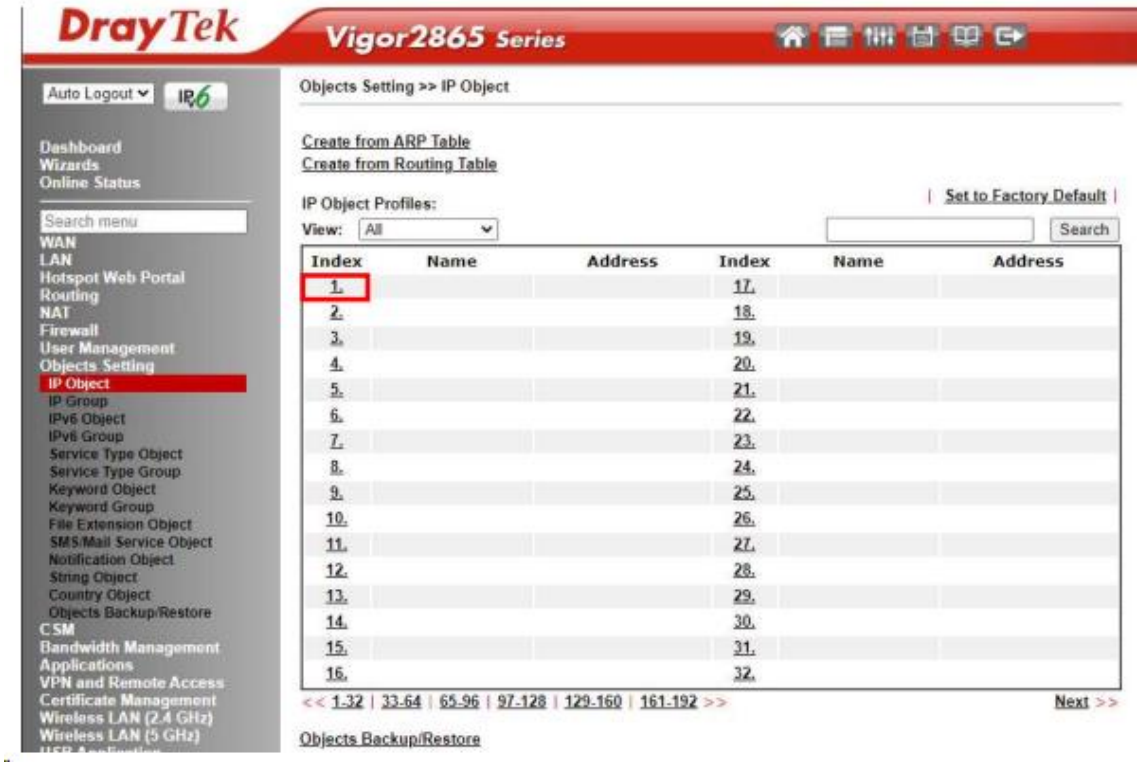
-77.239.128.0/24

Account VoIP "sip.voipvoicetel.it"

-212.97.59.64/27 -193.227.104.0/24 -109.233.128.0/21 -93.94.93.0/24

Per utilizzare tutti questi range di indirizzi IP in una sola regola, occorrerà creare un "IP Object" per ogni subnet.

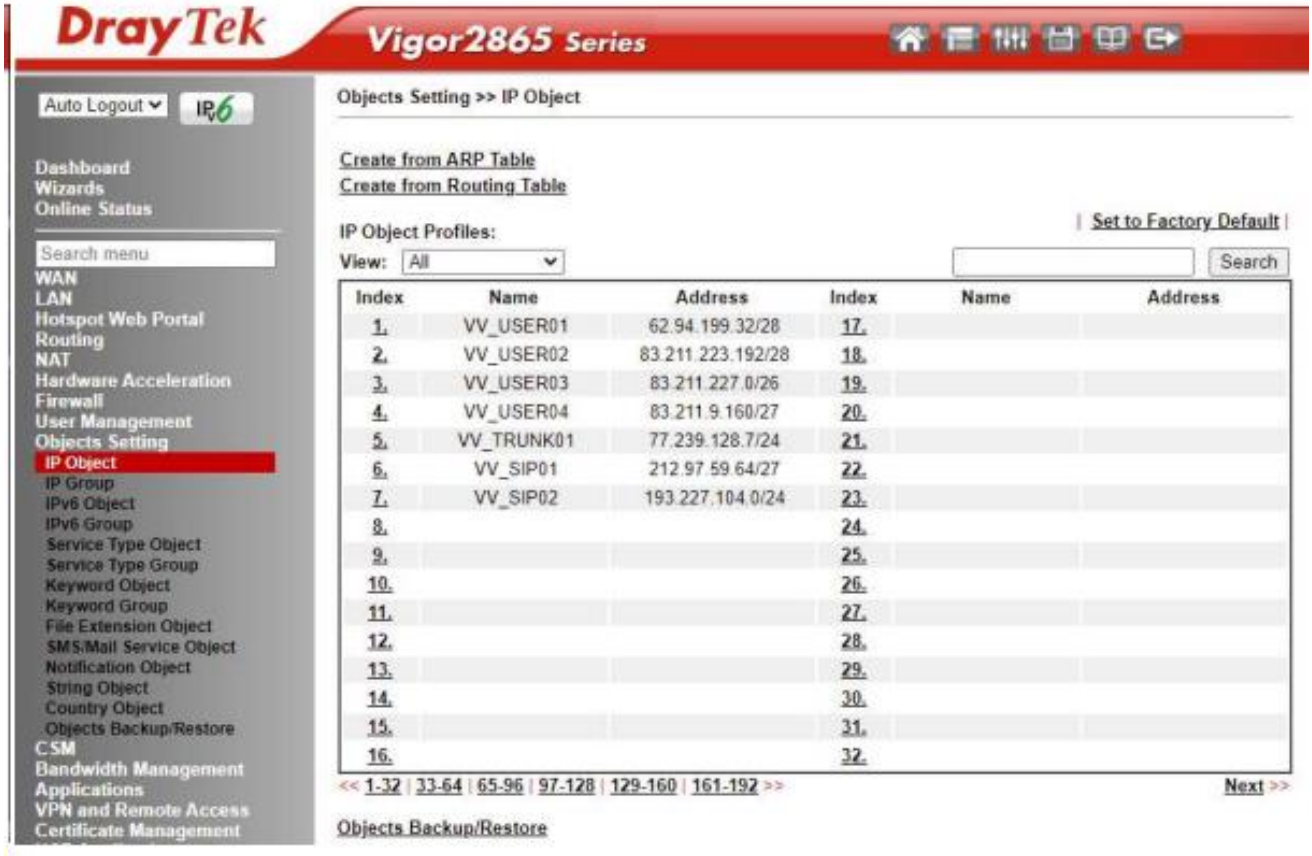
Dal menu Object Setting → IP Object, inseriamo manualmente i 7 range di IP Voipvoice. Ovviamente, nel caso in cui si utilizzi una sola tipologia di account VoIP VoipVoice, sarà possibile inserire una sola subnet oppure fino a 4 subnets. Nel nostro esempio andremo ad inserire tutte e 7 le subnet, cliccando prima sull'index 1.



Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

Procedere inserendo singolarmente tutte le regole come illustrato in questo esempio:

Al termine dell'inserimento avremo la seguente situazione:

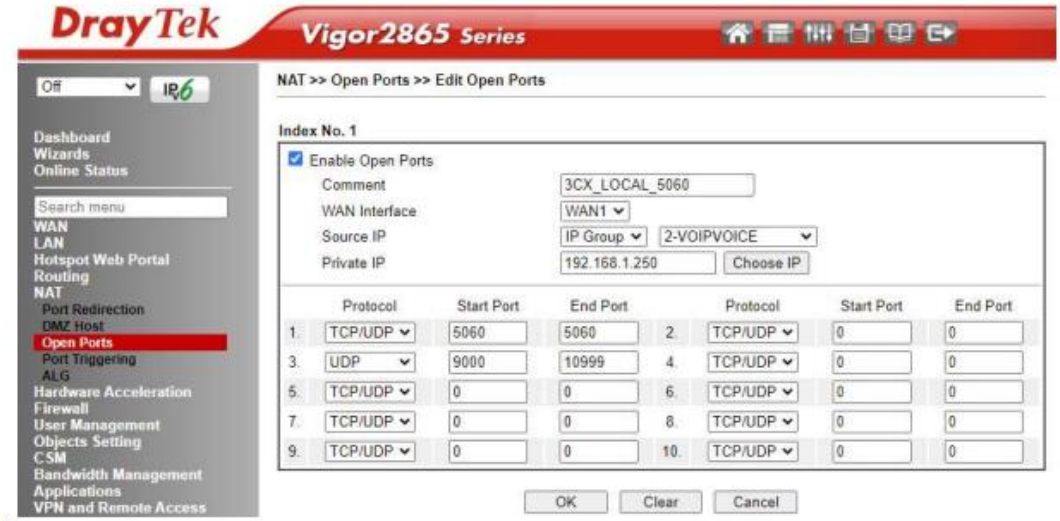


Guida alla Configurazione NAT e ACL con PBX su Draytek 2765/2865/2927/2962

Una volta creati i singoli oggetti procederemo a creare il gruppo di oggetti nel menu Objects Setting → IP Group.

Aggiungeremo, come index 1, il gruppo “VOIPVOICE”, selezionando tutti gli indirizzi disponibili e spostandoli nella colonna di destra.

Affinché le regole ACL siano applicate a livello di NAT è sufficiente accedere al menu NAT → “Open Ports”, richiamare la regola 1, creata in precedenza e alla voce “Source IP” selezionare IP Group e quindi “VoipVoice”



In questo specifico caso, la regola di NAT sarà applicata per le porte 5060 e il range 10000-20000. Il NAT sarà però protetto e applicabile solo per gli Indirizzi WAN appartenenti alle subnet VoipVoice.

Nessun dispositivo esterno, salvo gli indirizzi IP appartenenti alla subnet VoipVoice, potrà contattare il Centralino IP sulla porta TCP/UDP 5060 e sulle porte 10000-20000.

(Le porte 5060,10000-20000 sono usate come esempio, le porte abilitate saranno quelle indicate precedentemente nella configurazione della parte NAT).